AMENDMENTS TO THE CLAIMS

The following listing of claims replaces all prior listings of claims:

Listing of Claims:

1. (Currently Amended) A method, comprising:

receiving a second data record to be stored on a single database, wherein the database comprises a first data record;

storing the second data record on the database, wherein the second data record is stored consecutive to the first data record;

retrieving a first integrity checksum stored with the first data record previous to the second data record;

computing a second integrity checksum for the second data record with a cryptographic method using a storage key, the retrieved first integrity checksum and the second data record, wherein the storage key represents an identity of a signing entity authorized to sign data records;

storing the second integrity checksum on the database; and

configuring the retrieved integrity checksum for a first row of the database to be a generated initialization vector or a digital signature of a signing entity.

2. (Previously Presented) The method according to claim 1, further comprising:

configuring the storage key to be a secret key of public key infrastructure.

3-4 (Cancelled)

5. (Previously Presented) The method according to claim 1, wherein the retrieving the first integrity checksum comprises retrieving the first integrity checksum from a memory of a signing entity.

6. (Previously Presented) The method according to claim 1, further comprising:

storing the second integrity checksum on a memory of a signing entity.

7. (Previously Presented) The method according to claim 1, further comprising:

configuring the integrity checksums to comprise a running sequence number.

8. (Currently Amended) A method, comprising:

retrieving a second data record to be verified from a single database;

retrieving a second integrity checksum of the second data record, wherein the first data record and the second data record are consecutive data records in the database;

retrieving a first integrity checksum of the first data record previous to the retrieved second data record;

computing a third integrity checksum for the second data record based-musing the retrieved second data record, the first integrity checksum, and a storage key, wherein the storage key represents an identity of a signing entity authorized to sign data records;

comparing the second integrity checksum to the third integrity checksum, wherein the second data record is considered authentic when the second integrity checksum and the third integrity checksums are equal; and

configuring the retrieved integrity checksum for a first row of the database to be a generated initialization vector or a digital signature of a signing entity.

9. (Previously Presented) The method according to claim 8, further comprising:

configuring the storage key to be a public key of public key infrastructure.

10-11 (Cancelled)

12. (Previously Presented) The method according to claim 8, wherein the retrieving the first integrity checksum comprises retrieving the first integrity checksum from a memory of a verification entity.

13. (Previously Presented) The method according to claim 8, further comprising:

storing the second integrity checksum on a memory of a verification entity.

14. (Previously Presented) The method according to claim 8, further comprising:

configuring the integrity checksums to comprise a running sequence number.

15. (Currently Amended) A system, comprising:

a single database configured to store and provide signed data;

a data source configured to provide data records to be stored on the database;

a signing entity configured to sign data records to be stored on the database system with a second integrity checksum computed using a second data record, a first integrity checksum of the first data record previous to the second data record to be signed, and a storage key, wherein the first data record and the second data record are consecutive data records in the database, wherein the storage key represents an identity of a signing entity authorized to sign data records; and

a verification entity configured to verify integrity of chosen data records by computing a computed third integrity checksum using the second data record, the first integrity checksum of the first data record previous to the second data record, and the storage key, and comparing the computed third integrity checksum to the second integrity checksum stored on the database.

16. (Previously Presented) The system according to claim 15, wherein the signing entity and verification entity are configured to apply public key infrastructure to

calculate and verify at least one of the first integrity checksum or the second integrity checksum.

17. (Currently Amended) A ~~computer program embodied on a~~ computer-readable storage medium including a ~~, wherein the~~ computer program which when executed performs a process comprising ~~the following, when executed in a computer device~~:

receiving a second data record to be stored on a single database, wherein the database comprises a first data record;

storing the second data record on the database, wherein the second data record is stored consecutive to the first data record;

retrieving a first integrity checksum stored with the first data record previous to the second data record;

computing a second integrity checksum for the second data record with a cryptographic method using a storage key, the retrieved first integrity checksum and the second data record, wherein the storage key represents an identity of a signing entity authorized to sign data records;

storing the second integrity checksum on the database; and

configuring the retrieved integrity checksum for a first row of the database to be a generated initialization vector or a digital signature of a signing entity.

18. (Currently Amended) The ~~computer program~~ computer-readable storage medium according to claim 17, wherein the storage key is a secret key of public key infrastructure.

19-20 (Cancelled)

21. (Currently Amended) The ~~computer program~~ computer-readable storage medium according to claim 17, wherein the first integrity checksum is retrieved from a memory of the signing entity.

22. (Currently Amended) The ~~computer program~~ computer-readable storage medium according to claim 17, wherein the second integrity checksum is stored on a memory of the signing entity.

23. (Currently Amended) The ~~computer program~~ computer-readable storage medium according to claim 17, wherein the integrity checksums comprise a running sequence number.

24. (Currently Amended) A ~~computer program embodied a~~ computer-readable storage medium including a ~~, wherein the~~ computer program which when executed performs a process comprising ~~the following, when executed in a computer device~~:

retrieving a second data record to be verified from a database;

retrieving a second integrity checksum of the second data record to be verified from a database;

retrieving a first integrity checksum of a first data record previous to the retrieved second data record, wherein the first data record and the second data record are consecutive data records in the database;

computing a third integrity checksum for the second data record using the retrieved second data record, the first integrity checksum, and a storage key, wherein the storage key represents an identity of a signing entity authorized to sign data records; and

comparing the second integrity checksum to the third integrity checksum, wherein the second data record is considered authentic when the second integrity checksum and the third integrity checksums are equal; and

configuring the retrieved integrity checksum for a first row of the database to be a generated initialization vector or a digital signature of a signing entity.

25. (Currently Amended) The ~~computer program~~ computer-readable storage medium according to claim 24,

wherein a storage key is a public key of public key infrastructure.

26-27 (Cancelled)

28. (Currently Amended) The ~~computer program~~ computer-readable storage medium according to claim 24, wherein the first integrity checksum is retrieved from a memory of a verification entity.

29. (Currently Amended) The ~~computer program~~ computer-readable storage medium according to claim 24, wherein the second integrity checksum is stored on a memory of a verification entity.

30. (Currently Amended) The ~~computer program~~ computer-readable storage medium according to claim 24, wherein the integrity checksums comprise a running sequence number.

31. (Currently Amended) A system, comprising:

storage means for storing and providing signed data, wherein the storage means is singular;

provision means for providing data records to be stored on the storage means;

signing means for signing data records to be stored on the storage means with a second integrity checksum computed using a second data record, a first integrity checksum of the first data record previous to the second data record to be signed, and a storage key, wherein the first data record and the second data record are consecutive data records in the database, wherein the storage key represents an identity of a signing entity authorized to sign data records; and

verification means for verifying integrity of chosen data records by computing a computed third integrity checksum using the second data record, the first integrity checksum of the first data record previous to the second data record, and the storage key, and comparing the computed third integrity checksum to the second integrity checksum stored on the storage means.

32. (Previously Presented) The system of claim 31, wherein the signing means and verification means are configured to apply public key means for calculating and verifying at least one of the first integrity checksum or the second integrity checksum.

33. (Currently Amended) An apparatus, comprising:

a receiver configured to receive a second data record to be stored on a single database, wherein the receiver is further configured to receive a first integrity checksum stored with a first data record previous to the second data record, wherein the first data record and the second data record are consecutive data records in the database;

a processor configured to compute a second integrity checksum for the second data record with a cryptographic method using a storage key, the received first integrity checksum and the second data record, wherein the storage key represents an identity of a signing entity authorized to sign data records; and

a memory configured to store the second data record and the second integrity checksum on the database, wherein the second data record is stored consecutive to the first data record,

wherein the retrieved integrity checksum for a first row of the database is configured to be a generated initialization vector or a digital signature of a signing entity.

34. (Previously Presented) The apparatus of claim 33, wherein the storage key is configured to be a secret key of public key infrastructure.

35-36 (Cancelled)

37. (Previously Presented) The apparatus of claim 33, wherein the first integrity checksum is received from a memory of a signing entity.

checksums comprise a running sequence number.

38. (Previously Presented) The apparatus of claim 33, wherein the integrity checksums comprise a running sequence number.

39. (Currently Amended) An apparatus, comprising:

a receiver configured to receive a second data record to be verified from a single database, wherein the receiver is also configured to receive a second integrity checksum of the second data record, wherein the first data record and the second data record are consecutive data records in the database, and wherein the receiver is further configured to receive a first integrity checksum of a first data record previous to the received second data record;

a processor configured to compute a third integrity checksum for the second data record using the received second data record, the first integrity checksum, and a storage key, wherein the processor is further configured to compare the second integrity checksum to the third

integrity checksum, wherein the second data record is considered authentic when the second integrity checksum and the third integrity checksums are equal, wherein the storage key represents an identity of a signing entity authorized to sign data records,

wherein the retrieved integrity checksum for a first row of the database is configured to be a generated initialization vector or a digital signature of a signing entity.

40. (Previously Presented) The apparatus of claim 39, wherein the storage key is configured to be a public key of public key infrastructure.

41-42 (Cancelled)

43. (Previously Presented) The apparatus of claim 39, wherein the first integrity checksum is received from a memory of a verification entity.

44. (Previously Presented) The apparatus of claim 39, wherein the integrity checksums comprise a running sequence number.